

**DEPARTMENT OF THE NAVY  
NAVAL POSTGRADUATE SCHOOL  
MONTEREY, CALIFORNIA 93943-5101**

**FAR PART 13.5  
TEST PROGRAM FOR CERTAIN COMMERCIAL ITEMS  
JUSTIFICATION AND APPROVAL  
FOR USE OF SOLE SOURCE**

**1. Contracting Activity.**

NAVSUP FLC San Diego

**2. Description of the Action Being Approved.**

This justification and approval covers the procurement of software development support services for the Naval Postgraduate School by Other Than Full and Open Competition from Via Forensics. This effort will create a software library and tool for extracting files and other information from telephones running the Android operating system. The base period of performance for this proposed action acquisition is for one year. The software will enable The Sleuth Kit to read YAFFS2 file systems. Work includes the creation of releasable test data and the development of regression testing software.

The software will be delivered in source code form that will compile on Fedora Core 15 Linux, Ubuntu 11.04 Linux, Macintosh OS 10.6, and Windows using the mingw32 and mingw64 cross-compiler environments. Included with the software will be redistributable memory dumps from a variety of Android telephones and a command-line program for automated regression testing and validation. The initial version of the software shall extract resident files. Subsequent versions will be able to recover metadata from deleted files and eventually intact data from deleted files (ie: data that has not yet been overwritten during the course of flash garbage collection.).

The software will be delivered to the government with all data rights as either public domain or open source software with a license approved by the Open Source Initiative.

**3. Description of Supplies/Services.**

Open Source software to enable the Sleuth Kit to read YAFFS2 file systems; releasable test data and the development of regression testing software to be delivered in the aforementioned source codes.

**4. Statutory Authority Permitting SOLE SOURCE.**

Section 4202 of the Clinger-Cohen Act of 1996 - a sole source acquisition under the authority of the test program for certain commercial items, as implemented by FAR 13.501(a).

10 U.S.C. 2304 (c)(1) – Only one responsible source and no other supplies or services will satisfy agency requirements.

**5. Rational Justifying Use of Cited Statutory Authority.**

Pursuant to FAR 6.302-1(a)(2)(iii), this authority is appropriate when services are deemed to be available only from the original source and a follow-on contract for the continued provision of

highly specialized services is necessary. It is likely that award to any other source would result in unacceptable delays in fulfilling the agency's requirements. (See 10 U.S.C. 2304(d)(1)(B).)

This project builds upon previous work at the Naval Postgraduate School and a presentation that Mr. Hoog made on July 12, 2011 at the invitation of NPS, as well as the textbook *Android Forensic: Investigation, Analysis and Mobile Security for Google Android* (ISBN 1597496510) published in June 2011 by Mr. Hoog. NPS will leverage work previously done by Mr. Hoog to achieve the end result, a software library and tool that can be used at NPS and by other US Government agencies. The overall goal is to create and distribute a software package that can be used for reconstructing files and other information from physical memory dumps taken from Android phones. Mr. Hoog's expertise and extensive knowledge of the Android platform and mobile security is necessary for the development of the deliverable. Any other source would result in delays for the government in creating this technology.

ViaForensics is the leader in Android forensics and are currently the experts in the following fields:

- Android data recovery and analysis, including deleted information
- Recovering Android SMS / text messages
- Recovering contacts and other data from Android devices
- Recovering emails sent or received on Android phones
- Motorola Droid forensics, as well as G1, HTC Eris, and more
- Analyzing GPS information
- Advanced Android phone forensics

Simson Garfinkel will be working with Andrew Hoog, Chief Investigative Officer and co-founder of ViaForensics. Andrew Hoog is a computer scientist, certified forensic analyst (GCFA and CCE), computer and mobile forensics researcher, author of two forensic and security books, and expert witness. He has two patents pending in the areas of forensics and data recovery.

#### **6. Description of Efforts Made to Solicit Offers from as Many Offerors as Practicable.**

Support for the YAFFS2 file system as an enhancement to the Sleuth Kit was advertised publicly on the Forensics Wiki with inadequate response. After conducting further market research, the requirement has been found to be sole source for ViaForensics. No other vendor possesses the knowledge or expertise in the Android market required for the scope of the project. ViaForensics is the leader in Android Mobile Forensics.

#### **7. Unusual and Compelling Urgency.**

The Sleuth Kit is widely used within the US Government and the Department of Defense as the basis of systems that perform automated computer forensic processing. Currently The Sleuth Kit does not support the YAFFS2 file system used by modern Android Smart Phones. Increasingly Android phones are being acquired by the US Department of Defense in a variety of conflicts. The Sleuth Kit must be extended to include support for YAFFS2 if we are to process Android systems using automated means built on top of The Sleuth Kit. There is currently no project underway that will add support for YAFFS2 to The Sleuth Kit in a timely manner.

#### **8. Determination of Fair and Reasonable Cost.**

Dr. Simson Garfinkel used his knowledge of software engineering and computer forensics in the preparation of the Independent Government Estimate. An Independent Government Estimate (IGE) has been provided and the Contract Specialist will use this to determine price reasonableness. The determination of fair and reasonable is based primarily labor hours, material, and other overhead costs to meet the exact specifications of the government. The placement of a firm, fixed price order is anticipated.

**9. Actions to Remove Barriers to Future Competition.**

The results of this contract will be publicized at conferences and published in academic journals. Open source software resulting from this contract will be made freely available. Others in academia and the corporate world will be free to build upon it.

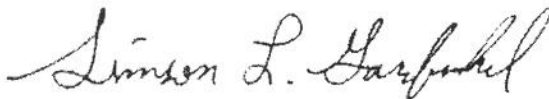
## CERTIFICATIONS AND APPROVAL

### TECHNICAL/REQUIREMENTS CERTIFICATION

I certify that the facts and representations under my cognizance which are included in this Justification and its supporting acquisition planning documents, except as noted herein, are complete and accurate to the best of my knowledge and belief.

#### Technical Cognizance:

Signature:



Date:

August 8, 2011

#### Requirements Cognizance:

Signature: \_\_\_\_\_

Date:

(Note that this page includes certification that the acquisition planning documents are complete and accurate.)

(If a single individual has cognizance over both technical and requirements information included in the J&A, use of only one signature line is encouraged ["Technical Cognizance:" and Requirements Cognizance:" may also be deleted]).

### LEGAL SUFFICIENCY REVIEW

I have determined this Justification is legally sufficient.

Signature

Name (Printed)

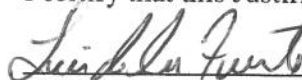
Phone No.

Date

### CONTRACTING OFFICER CERTIFICATION

(\$150K - \$550K)

I certify that this Justification is accurate and complete to the best of my knowledge and belief.

 LUIS DELAFUENTE 8/16/11 619-532-2889

Signature

Name (Printed)

Phone No.

Date